EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ficpro.com.br	Checks	9 pruebas
Dominio	ficpro.com.br	Hallazgos	44 totales
Fecha	27 de marzo de 2026 a las 10:55	Problemas	17 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 75/100, otorgando una calificación global de B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 finalizaron correctamente y 3 presentaron fallos críticos que comprometen la infraestructura. Aunque la capa de transporte y el cifrado de datos son robustos, la exposición de servicios internos y la falta de cabeceras de seguridad representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable debido a una superficie de ataque excesivamente amplia en el servidor. El éxito de un posible ataque es elevado si no se mitigan las aperturas de puertos detectadas.

Resumen de Riesgos

6	3	6	2	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	9 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 67 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  67 dias restantes (expira: 2026-06-02T18:07:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-04T18:07:01.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Netlify — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://ficpro.com.br/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 20/100

Estado: FALLO

9 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- CRITICO **Puerto 23 (Telnet)**
  ABIERTO — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- CRITICO **Puerto 27017 (MongoDB)**
  ABIERTO — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 23 (Telnet): ABIERTO — Acceso remoto sin cifrar que permite la interceptación de credenciales.
[CRITICAL] Puerto 3306 (MySQL): ABIERTO — Base de datos MySQL expuesta directamente a internet, vulnerable a ataques de fuerza bruta.
[CRITICAL] Puerto 3389 (RDP): ABIERTO — Interfaz de escritorio remoto de Windows accesible, objetivo principal para ransomware.
[CRITICAL] Puerto 5432 (PostgreSQL): ABIERTO — Base de datos PostgreSQL expuesta, facilitando intentos de acceso no autorizado.

[CRITICAL] Puerto 6379 (Redis): ABIERTO — Sistema de caché que suele carecer de autenticación por defecto, permitiendo la extracción de datos.
[CRITICAL] Puerto 27017 (MongoDB): ABIERTO — Base de datos NoSQL expuesta que podría permitir el borrado o secuestro de información.
[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de código.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking al permitir ser cargado dentro de frames externos.
[HIGH] Puerto 21 (FTP): ABIERTO — Protocolo de transferencia de archivos inseguro que transmite datos y contraseñas en texto plano.
[MEDIUM] Referrer-Policy: Falta — No se controla la cantidad de información que el navegador envía al navegar hacia otros enlaces.
[MEDIUM] Permissions-Policy: Falta — Ausencia de restricciones sobre el uso de APIs del navegador como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html y /README.txt: Accesibles — Estos archivos pueden revelar metadatos sobre la tecnología y versiones utilizadas.
[MEDIUM] Puerto 22 (SSH): ABIERTO — Servicio de administración remota expuesto que requiere endurecimiento de seguridad.
[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — Puerto alternativo que suele alojar paneles de administración o servicios secundarios sin proteger.
[LOW] Server header expuesto: Netlify — Revela información sobre la infraestructura que ayuda a un atacante a dirigir sus esfuerzos.
[LOW] X-Powered-By expuesto: Next.js — Divulga el framework utilizado, permitiendo la búsqueda de vulnerabilidades específicas de la versión.